REMARKS

In the Office Action, the Examiner noted that Claims 1 through 9 were pending in the Application. The Examiner rejected all claims. Claim 1 has been amended to describe that the certificate is stored on computer readable medium, Claim 7 has been amended to correct an informality in the claim, and new Claims 10 - 12 have been added. Thus, Claims 1 - 12 are pending in the Application. Applicant traverses the rejections below.

I. Traversal of the Rejection over the Cited Art

The Examiner rejected Claims 1 through 6 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,923,756 to Shambroom and passages from the Schneier book "Applied Cryptography" in view of U.S. Patent No. 6,157,721 to Shear et al. Applicant traverses this rejection below.

A. The Present Invention

The present invention discloses an extended X.509 certificate capable of supporting more than one cryptographic algorithm. The certificate comprises a signature algorithm and a signature for all authenticated attributes using a first cryptographic algorithm, and alternative public key extension for identifying at least one alternative cryptographic algorithm and providing its associated public key, and an alternative signature extension for containing a signature for the alternative cryptographic algorithm.

B. Differences Between the Present Claims and the Cited Art

The Office Action identifies a passage from Shambroom as disclosing "a certificate that supports one or more cryptographic algorithms" and that "the certificate can resemble an X.509 certificate," citing Column 10, lines 32-35

More specifically, Shambroom states that "web server 720 responds with a certificate to web browser 620. This certificate contains the network server's public key and a list of one or more cryptographic algorithms that the network server supports..." (Column 10, lines 30-34).

The key here is that the Shambroom certificate contains a **list** of one or more cryptographic algorithms that the **network server** supports. The Shambroom certificate does not actually use or employ multiple cryptographic algorithms to protect the data therein. The Shambroom data appears to be the list of algorithms. The certificate in Claim 1 does **not** contain a list of cryptographic algorithms that a network server supports. The claimed certificate utilizes and uses more than one cryptographic algorithm itself to protect the data it includes.

Further, the network server's public key appears to be used by the web browser to log onto or communicate with the web server 720, which is part of the network server 700, and not to protect the data in the certificate. In other words, the Shambroom certificate is used to transfer data, including the list of cryptographic algorithms that the network server supports and the public key for the network server, to the web browser. No such scheme is contemplated by the present invention.

The Office Action goes on to state that the "list of algorithms disclosed in Shambroom also anticipates an extension for identifying at least one alternative algorithm." This statement is not supported by Shambroom. Shambroom does not mention certificate extensions. The Shambroom list is not a certificate extension. There is no mention that the list takes the form of a certificate extension. Rather, as discussed above, the list is data which is relevant to which algorithms the network server supports. They have nothing to do with protecting the information in the certificate, as per the claimed subject matter.

Claim 1 recites that the X.509 certificate comprises "a signature algorithm and signature for all authenticated attributes using a first cryptographic algorithm;" as well as "an alternative public key extension for identifying at least one alternative cryptographic algorithm and

providing its associated public key; and an alternative signature extension for containing a signature for the alternative cryptographic algorithm." This is not the same thing as a list of cryptographic algorithms that a network server supports as per Shambroom, and such a list included in a certificate does not teach, suggest or disclose the subject matter of Claim 1. Shambroom does not teach that its certificate protects its data using more than one cryptographic algorithm. The Shambroom list appears to be data included in the certificate, not multiple cryptographic algorithms employed by the certificate to protect its data, as per Claim 1.

Schneier appears to describe a standard X.509 certificate which employs a single cryptographic algorithm. Applicant notes that portions of pages 480, 481, 574 and 575 of Schneier were not legible in the photocopies provided with the Office Action.

Including a list of cryptographic algorithms as data in a certificate does not teach, suggest or disclose using multiple algorithms to protect the data in the certificate. There is no reason to combine Shambroom's list of cryptographic algorithms contained in a certificate (which indicate which algorithms a server supports) with the standard X.509 certificate, such as that of Schneier, which actually uses a single algorithm to protect data contained therein.

The current Office Action also uses the Shear reference in rejecting Claim 1. Shear is directed to security for load modules. In the Abstract, Shear states that the use of "several dissimilar digital signature algorithms may be used to reduce vulnerability from algorithm compromise, and subsets of multiple digital signatures may be used to reduce the scope of any specific compromise."

However, Shear does not suggest, teach or disclose creating extensions to a certificate. The Office Action argues that it would be obvious to put multiple signatures formed with different algorithms into Shambroom's certificate based on the teachings of Shear.

Applicant has never argued that the present invention claims the concept of using more

than one algorithm for the purpose of security. Rather, Applicant has figured out how to make such a multiple algorithm system work with respect to certificates. This involves the use of extensions. And none of the references teaches this or mentions the use of extensions in such a manner. None of Shambroom, Shear and Schneier discusses the use of extensions to enable the certificate to support an alternative cryptographic algorithm, as per the second and third elements of Claim 1.

Accordingly, Applicant submits that Claim 1 patentably distinguishes over the combination of Shambroom, Shear and Schneier. Accordingly, dependent Claim 2 and 3 should also distinguish over the cited art. While the subject matter of independent Claim 4 and dependent Claims 5 and 6 were not specifically addressed in the discussion under numbered paragraph 11, they were rejected for the same reasons as Claims 1 - 3, and thus should patentably distinguish over the cited art for the same reasons as Claim 1 - 3 do. Claims 7 - 12 should also distinguish over the cited art for the same reasons as provided above.

C. Response to Arguments in Office Action

In numbered paragraph 4 of the Office Action, the Examiner noted that "one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references." On some level, this may be true. However, if an applicant can show that a given reference does not in fact teach, suggest or disclose those portions of the claims that the reference is utilized in a rejection to teach, suggest or disclose, then the combination is improper and the obviousness rejection cannot stand. If individual references may not be attacked, then a reference directed to mousetraps could be combined with a reference directed to a semiconductor in order to render claims directed to bioengineered corn obvious with neither the semiconductor reference nor the mousetrap reference being 'attackable' individually. Certainly, each reference may be 'attacked' for not teaching, suggesting or disclosing what they are alleged to teach, suggest or show, thus rendering the scope of the combination incomplete relative to the claimed subject matter.

In numbered paragraph 3, the current Office Action argues that "the bits in Shambroom that identify the cryptographic algorithms, which are additional information, read on an extension." What this discussion shows is that the Office Action is taking little bits and pieces out of the various cited references and combining them in a way not contemplated by the references as a collection and without an teaching to combine the references in the manner combined. Are "bits" from Shambroom to which the Office Action is referring to the "list" of algorithms. An extension is a well-defined term of art in the certificate art. The addition of bits to a list of algorithms does not teach, suggest or disclose adding an extension to a certificate.

The prior Office Action, it was argued in numbered paragraph 3 that the fact that the "present invention does not transfer data that includes a list of cryptographic algorithms" does not matter, because "applicant has recognized another advantage which would flow naturally from following the suggestion of the prior art..." Applicant has made no such recognition. As discussed above, a list of algorithms does not anticipates an extension for identifying at least one alternative algorithm. The argument in paragraph 3 is not supported by Shambroom. Shambroom does not mention certificate extensions. The Shambroom list is not a certificate extension. There is no mention that the list takes the form of a certificate extension. Rather, as discussed above, the list is data which is relevant to which algorithms the network server supports. They have nothing to do with protecting the information in the certificate, as per the claimed subject matter.

In numbered paragraph six, the Office Action states that the combination of references is proper because "Shear et al, while specifically directed to load modules, executables, and other data elements teaches multiple signatures created with dissimilar algorithms in a broadly applicable fashion, and thus the combination is proper." As noted above, the most pertinent passage of Shear states, in the Abstract, that the use of "several dissimilar digital signature algorithms may be used to reduce vulnerability from algorithm compromise, and subsets of multiple digital signatures may be used to reduce the scope of any specific compromise." Shear is directed to security for load modules. There is nothing in the art that suggests the desirability to

combine the references. Shear is directed to load modules and executables, not certificates. The ability to enable a certificate to support more than one cryptographic algorithm is an entirely different problem.

In numbered paragraph seven, the Office Action erroneously states that "applicant agrees that the claims recite data." What Applicant stated is that the claims recite functional structure for data, much like Shear. It is interesting that the Office Action goes on to state that Shear claims physical objects. If this is the case, then Shear clearly cannot be combined with the other references, as the other references are not directed to physical objects. However, Applicant believes Shear to be directed to code, and the barrier, arrangement and load module of Shear's claim 14 are certainly not a physical barrier, a physical arrangement and a physical load module, but functional structures for data. Physical names have been provided to these structural elements which are purely code based.

D. Improper Combination of References

Additionally, the Examiner has failed to provide a convincing line of reasoning for combining the teachings and structure of Shambroom with the teachings and structure of Schneier and the teachings and structure of Shear so as to arrive at the present claimed invention. Under 35 U.S.C. Section 103, when the Examiner has relied on the teachings of several references, the test is whether or not the references viewed individually and collectively would have suggested the claimed invention to the person possessing ordinary skill in the art. See In re Kaslow, 707 F.2d 1366, 217 USPQ 1989 (Fed. Cir. 1983). It is to be noted, however, that citing references which merely indicate that isolated elements and/or features recited in the claims are known is not a sufficient basis for concluding that a combination of claimed elements would have been obvious. That is to say, there should be something in the prior art or a convincing line of reasoning suggesting the desirability of combining the references in such a manner as to arrive at the claimed invention. See In re Deminski, 796 F.2d 436, 230 USPQ 313 (Fed. Cir. 1986).

Applicants submit that there is no teaching in the reference or a convincing line of reasoning provided by the Examiner to combine the teachings of Shambroom, Shear and Schneier so as to arrive at the present claimed invention. Shambroom discloses a certificate that contains a **list** of one or more cryptographic algorithms that a **network server** support. Schneier describes a standard X.509 certificate which employs a single cryptographic algorithm. Shear is directed to security for load modules which uses several dissimilar digital signature algorithms. No reason is provided for combining a certificate which carries a list of algorithms (Shambroom) with a standard X.509 certificate (Schneier) with the concept that multiple dissimilar digital signature algorithms may be used for security for load modules. How and why anyone would combine these references so as to arrive at the present claimed invention is entirely unclear. Certainly, nothing is provided in the references that would suggest combining these references. No appropriate line of reasoning is provided for combining these references. Accordingly, Applicant submits that the combination of references is inappropriate and improper and respectfully submit that this is a further reason to overturn the rejection that stands alone from the reasons discussed above relative to the content of the references.

II. Traversal of the Rejection under 35 U.S.C. Section 101

Claims 1 - 3 were rejected under 35 U.S.C. Section 101 for being directed to non-statutory subject matter. The rejection states that the claims claim data.

Claim 1 has been amended to recite that the certificate is stored on computer readable medium.

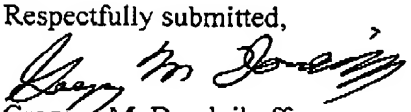
Applicant submits that the claims are statutory. The claims recite a functional structure for data. The claims do not recite sales data or a list of addresses. For example, in the Shear patent cited by the Examiner, Claims 14 and 34 recite a security structure. The barrier, arrangement and load module of Shear's claim 14 are certainly not a physical barrier, a physical arrangement and a physical load module, but functional structures for data.

If the position of the USPTO is that these claims of Shear are non-statutory, since the Office has been placed on notice that the claims exist in an issued patent, then the Office should attempt to recall the issued patent, as it has done for other recent patents, or the format will be considered valid not only under existing law but by estoppel as well. Since issued claims exist under the format, the USPTO would be estopped from taking a different position on subsequent claims.

III Summary

Applicant has presented technical explanations and arguments fully supporting their position that the pending claims contain subject matter which is not taught, suggested or disclosed by Shambroom, Schneier, or any combination thereof. Accordingly, Applicant submits that the present Application is in a condition for Allowance. Reconsideration of the claims and a Notice of Allowance are earnestly solicited.

Respectfully submitted,



Gregory M. Doudnikoff
Attorney for Applicant
Reg. No. 32,847

GMD:ld

Docket No: CR9-98-095
PHONE: 919-254-1288
FAX: 919-254-4330